

Security Management for ECLI, NETCONF, and File Transfer Protocols

DESCRIPTION

Copyright

© Ericsson AB 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Functions and Concepts	3
2.1	ECLI, NETCONF, and FTP Server IP Address	3
2.2	Session Parameters	4
2.3	SSH Authentication	4
2.4	TLS Authentication	5
2.5	SSH and TLS Transport Protocol Security	5
2.6	Types of Operations	5
3	Managed Object Model	9
4	Configuration Management	11





1 Introduction

This document provides an overview of the management model and concepts associated with the System Management and Security Management managed areas for Ericsson Command-Line Interface (ECLI) and NETCONF.

A managed area is represented by a group of Managed Object Classes (MOCs) within the Managed Object Model (MOM).



2 Functions and Concepts

An overview of Security Management is shown in Figure 1.

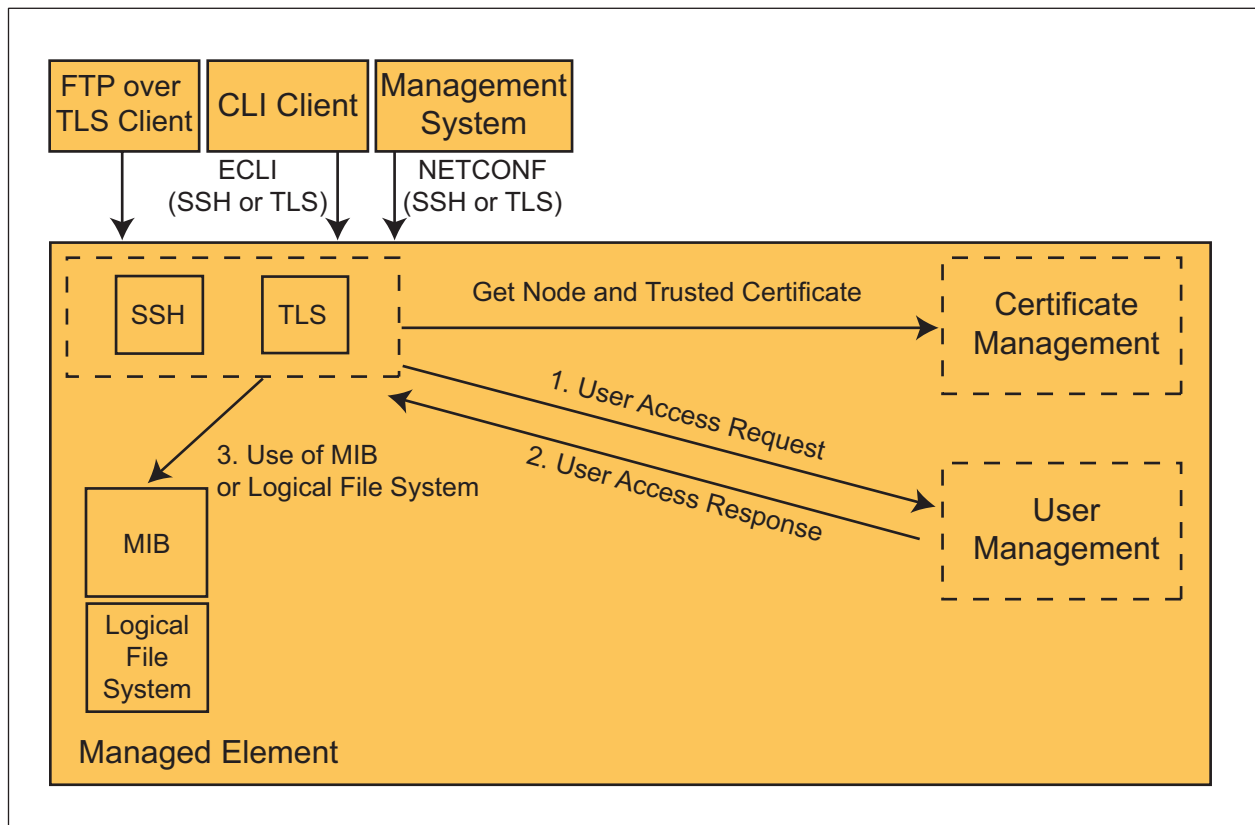


Figure 1 Security Management Overview

2.1 ECLI, NETCONF, and FTP Server IP Address

The IP address used for Operation and Maintenance (OAM) connections is defined at site deployment.

The ECLI, NETCONF, and FTP listen on all network addresses that are configured on the OAM processor.

The default port numbers for the OAM protocols are described in Table 1.

Table 1 Port Numbers of OAM Protocols

Service Name	SSH Port	TLS Port
ECLI	22	6522



Service Name	SSH Port	TLS Port
NETCONF	830	6513
FTP	-	21

The FTP over TLS port number is configurable in the MOM; see Section 2.6 Types of Operations on page 5.

Note: ECLI and NETCONF port numbers are not configurable in the MOM.

2.2 Session Parameters

Idle OAM sessions are timed out. The default time-out values are described in Table 2.

Table 2 Time-Out Value for Idle Sessions

Service Name	Time-out (Seconds)
ECLI	120
NETCONF ⁽¹⁾	300
FTP	3600

(1) The timer is disabled for NETCONF notification sessions.

The FTP session idle time out is configurable in the MOM, see Section 2.6 Types of Operations on page 5.

Note: The ECLI and NETCONF timer values are not configurable in the MOM.

2.3 SSH Authentication

The SSH host key of the ECLI and NETCONF server is generated after installation.

The public key of the SSH key can be fetched from the filesystem by executing a serial console connection. The MOM does not support presenting the host key of the SSH server.

An ECLI or NETCONF SSH connection can be initiated and the presented fingerprint can be compared to the fingerprint of the public key copied from the node.

SSH requires the user to provide credentials at logon for user authentication. A valid account must exist and be accessible by the User Management function to authenticate the user identity successfully. The user credential can be either a password or a public key. For more information, refer to *User Management*.



2.4 TLS Authentication

A Transport Layer Security (TLS) connection requires the proper configuration of certificates by *Certificate Management*.

The server certificate for ECLI, NETCONF, or FTP access is enrolled by using Certificate Management; refer to *Install Node Credential Online*, *Install or Renew Node Credential by CSR*, and *Install or Renew Node Credential by PKCS 12*. If the certificate is enrolled, the *CliTls* or *NetconfTls* MO in *SysM* must be configured to use this credential.

For the authentication of client certificates, the ECLI, NETCONF, or FTP server needs at least one trusted certificate deployed by Certificate Management, and a configured trust category. If the trust category is prepared, the *CliTls* or *NetconfTls* MO in *SysM* must be configured to use this trust category.

In TLS case, the client certificate must contain an identity in the Subject Alternative Name (SAN) field of the client certificate for authorization. The value of the SAN should be one of the following:

- DirectoryName (the CN attribute value is used as user id)
- Othername

If the SAN field is not present, the TLS connection closes.

A valid account must be present and accessible by the User Management function to authorize the user identity successfully. For more information, refer to *User Management*.

2.5 SSH and TLS Transport Protocol Security

Transport security level is defined by the actual security algorithms used for key exchange, message authentication, and encryption. The ME has a default algorithm set, which can be changed as described in *SSH and TLS Protocol Management*.

2.6 Types of Operations

System and security management of ECLI and NETCONF supports the following operations for an administrator with the System Administrator role.

Certificate Management

Certificate management must be used to set up TLS for ECLI and NETCONF to deploy node credentials and trusted certificate categories.

- Configure Node Credential



To configure a node credential for ECLI or NETCONF, a node credential must be installed by one of the operations *Install Node Credential Online*, *Install or Renew Node Credential by CSR*, or *Install or Renew Node Credential by PKCS 12*. After the installation, the node credential can be configured for ECLI or NETCONF. Refer to *Configure Node Credential for ECLI, NETCONF, or FTP over TLS*.

- Configure Trust Category

To configure a trust category for ECLI or NETCONF, a trust category must be created with at least one trusted certificate installed following *Create Trust Category* or *Install Trusted Certificate*. After the installation, the trust category can be configured for ECLI or NETCONF. Refer to *Configure Trust Category for ECLI, NETCONF, or FTP over TLS*.

Administrative State

The administrative state of the ECLI and NETCONF transport protocols can be changed to lock unnecessary protocols and interfaces and to unlock the needed ones. SSH-based protocols are unlocked by default, TLS-based protocols can be unlocked after deploying certificates.

- Change Administrative State of ECLI or NETCONF over SSH

If ECLI or NETCONF over TLS is in operation, optionally the SSH interface for ECLI or NETCONF can be closed. This does not affect the OS shell SSH interface.

Refer to *Change Administrative State of ECLI or NETCONF over SSH*.

- Change Administrative State of ECLI or NETCONF over TLS

After certificate deployment ECLI or NETCONF over TLS, interfaces can be unlocked. The TLS interfaces can be locked again if necessary.

Refer to *Change Administrative State of ECLI, NETCONF, or FTP over TLS*.

Port Numbers

The listening server port numbers can be changed for some O&M services, for example, if needed for adaptation to security policies.

- Change Port Number of FTP over TLS

The system uses a default port for FTP over TLS. If necessary, the port number can be changed. Refer to *Change Port Number of FTP over TLS*.

Session Idle Timers

The default session idle timer can be changed for some O&M services, for example, if needed for adaptations to firewall policies. A timer value of zero



means that the connection waits indefinitely for activity over the connection, that is, it never times out.

- Change Session Idle Timer of FTP over TLS

The system uses a default session idle timer for FTP over TLS. The idle timer can be changed. Refer to *Change Session Idle Timer of FTP over TLS*.



3 Managed Object Model

The System Management managed area is represented in the *Managed Object Model (MOM)* as follows:

```
ManagedElement
+-SystemFunctions
  +-SysM
    +-CliSsh
    +-NetconfSsh
    +-CliTls
    +-NetconfTls
    +-FileTPM
      +-FtpServer
      +-FtpTlsServer
```

For general information about the MOM, MOCs, MOs, cardinality, and related concepts, refer to *Managed Object Model User Guide*.

The System Management MOCs are described in Table 3.

Table 3 System Management Managed Object Class Descriptions

Managed Object Class	Description
<i>SysM</i>	The root of the System Management model
<i>CliSsh</i>	The CLI configuration management service over SSH
<i>NetconfSsh</i>	The NETCONF configuration management service over SSH
<i>CliTls</i>	The ECLI configuration management service over TLS
<i>NetconfTls</i>	The NETCONF configuration management service over TLS
<i>FtpServer</i>	The general configuration management of file transfer protocols.
<i>FtpTlsServer</i>	The FTP over Transport Layer Security (TLS) server of the ME.





4 Configuration Management

System and security management for ECLI and NETCONF is accessed using NETCONF or the ECLI to manipulate the MIB.

The following operations, described in Operating Instructions using the ECLI, can be performed by an administrator with the System Security Administrator role:

Certificate Management

- *Configure Node Credential for ECLI, NETCONF, or FTP over TLS*
- *Configure Trust Category for ECLI, NETCONF, or FTP over TLS*

System Management

- *Change Administrative State of ECLI or NETCONF over SSH*
- *Change Administrative State of ECLI, NETCONF, or FTP over TLS*
- *Change Port Number of FTP over TLS*
- *Change Session Idle Timer of FTP over TLS*